10-2017

Bitcoins and other cryptocurrencies as property?

Kelvin F. K. LOW
Singapore Management University, kelvinlow@smu.edu.sg

Ernie G. S. TEO

DOI: https://doi.org/10.1080/17579961.2017.1377915

Legal Studies Research Paper

2017

Bitcoins and Other Cryptocurrencies As Property?

Kelvin FK Low* and Ernie Teo**

Singapore Management University School of Law Research Paper No. 21/2017

This is a pre-print manuscript of a paper forthcoming in (2017) 9.2 Law, Innovation and Technology. Please refer to the journal at http://www.tandfonline.com/loi/rlit20 for the final version.

Bitcoins & Other Cryptocurrencies as Property?

Kelvin FK Low* and Ernie GS Teo**

ABSTRACT

The hype over bitcoins has been compared to the tulip mania in 17th century Netherlands and it has spawned a host of similar cryptocurrencies. As it has gained in popularity, the law has approached the subject warily, mostly from a regulatory perspective. However, no comprehensive consideration of the fundamental nature of a bitcoin owner's private law relation to his/her/its bitcoins has been properly conducted. Whether or not bitcoins or other cryptocurrencies achieve mainstream adoption or remain of interest to only a niche audience, this question will inevitably have to be properly addressed. This paper proposes to consider if bitcoins might be recognised as the subject of property rights by Commonwealth courts and if so, what such rights ought to entail. It will begin with a careful consideration of the controversial question of the scope of the law of property before considering bitcoin's place within the law of property (if any). What is the meaning of property in the common law? What fundamental differences exist between tangible and intangible property? If ownership of bitcoins is worthy of protection, what shape should it take? It suggests that the common law adopts a more expansive view of property than civilian systems and that it is thus able to accommodate bitcoins and other cryptocurrencies within its law of property. However, owing to their unusual nature, legal rights to them must take on a unique and unorthodox form. The code underlying Bitcoin also poses particular challenges to the law which this paper also addresses.

* Associate Professor, School of Law, Singapore Management University.

** Research Scientist, IBM Research.

The authors would like to thank their research assistant, Tan Hong Liang Gabriel, for his research assistance and comments on earlier drafts of the paper, without which the paper could not have been written. The usual caveats apply.

This is a pre-print manuscript of a paper forthcoming in (2017) 9.2 Law, Innovation and Technology. Please refer to the journal at http://www.tandfonline.com/loi/rlit20 for the final version.

1. INTRODUCTION

Bitcoin was conceived by the pseudonymous[1] Satoshi Nakamoto in his seminal white paper[2] first published in 1 November 2008.[3] In the paper, Satoshi Nakamoto describes a cryptographic system for "electronic cash" in which payment transactions are verified on the basis of group consensus rather than through financial institutions serving as trusted third parties. According to Satoshi Nakamoto, the inherent weakness of a trust based model was that transactions are not completely irreversible. As such, financial institutions cannot avoid mediating disputes which "increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions."[4] If payment transactions are reversible, it also entails merchants undertaking the risk of non-performance on the part of their counterparties since apparent payments can be subsequently rescinded. Bitcoin was envisaged as "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[5] As a result of the central role played by cryptography in the system, bitcoin and its derivatives are known as cryptocurrencies. Once properly validated, bitcoin transactions are irreversible, or in the parlance of the bitcoin community, immutable.[6]

---

[1] The true identity of Satoshi Nakamoto has been much speculated but remains unknown. See, eg, Robert McMillan (7 March 2014), "Why Bitcoin Doesn't Want a Real Satoshi Nakamoto", *Wired* at https://www.wired.com/2014/03/bitcoin_satoshi/ (accessed 5 April 2017), Izabella Kaminska (7 May 2016), "Bitcoin: Identity Crisis", *Financial Times*, Andrew O'Hagan (30 June 2016), "The Satoshi Affair", *London Review of Books* at https://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair (accessed 5 April 2017).

[2] Satoshi Nakamoto (October 2008), "Bitcoin: A Peer-to-Peer Electronic Cash System" at https://bitcoin.org/bitcoin.pdf (accessed 5 April 2017).

[3] Benjamin Wallace (23 November 2008), "The Rise and Fall of Bitcoin", *Wired* at https://www.wired.com/2011/11/mf_bitcoin/ (accessed 5 April 2017).

[4] Satoshi Nakamoto, n 2, 1.

[5] Satoshi Nakamoto, *ibid*, 1.

[6] This carries implications for legal remedies if it is determined that legal rights attach to holding bitcoins, for which see below text accompanying nn 98-130.

This is a pre-print manuscript of a paper forthcoming in (2017) 9.2 Law, Innovation and Technology. Please refer to the journal at http://www.tandfonline.com/loi/rlit20 for the final version.

Unlike most prior forms of "electronic money",[7] the system is neither derived from[8] nor backed by[9] any fiat currency. Instead, individual bitcoins are first created in the system through a process called mining. This process is intimately connected to the verification process by which transfers are tracked within the system. Instead of a centralised ledger (or register), the bitcoin system employs a decentralised system of ledgers known as the blockchain. The blockchain is essentially a register containing information tracking the creation and transfer of bitcoins much like a bank ledger tracks payments between bank accounts. Unlike bank accounts, however, the blockchain is not maintained by a central authority but instead resides in thousands of computers throughout the world. These computers are connected over the Internet to other computers running the same software, creating a network. When the holder of a bitcoin wishes to make a payment in bitcoin, an instruction is sent to this network and the computers on the network (nodes) validate the transaction before it is added to the blockchain files sitting on all the computers in the network. The process of validation involves the solution of a complex mathematical puzzle by nodes operated by users known as miners. Although the puzzles are described as complex, "[i]n fact there is nothing complex about this process, and you can do this by hand without a calculator; it just deliberately takes many computational steps without shortcuts."[10] In essence, this

[7] These are essentially obligations to pay a certain sum denominated in some form of fiat currency. See, generally, David Kreltszheim, "The Legal Nature of 'Electronic Money'" (2003) 14 *Journal of Banking and Finance Law and Practice* 161; 261.

[8] As a matter of legal analysis, Satoshi Nakamoto's understanding of the role of banks in inter-bank payments is probably mistaken. The role of the so-called trusted third party arose out of the necessity to have a common debtor in order to effect an extinction and creation of bank money, which is essentially a debt. The trust inherent in these payments is in large part trust in the solvency of these third parties rather than trust that they are not mistaken since they usually have to bear the costs of their own mistakes. See Stephan Meder, "Giro Payments and the Beginnings of the Modern Cashless Payment System" in David Fox and Wolfgang Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (2016), 441. In bitcoins and cryptocurrencies, trust in the solvency of the debtor is replaced by faith that they will either keep their value or else grow in value.

[9] Banking regulations require financial institutions to back up their obligations with fiat currency.

[10] Anthony Lewis (1 September 2015), "A Gentle Introduction to Bitcoin", *Bits on Blocks* at https://bitsonblocks.net/2015/09/01/a-gentle-introduction-to-bitcoin/ (accessed 5 April 2017).

involves the miners' computers engaging in a guessing game and the odds of winning are dependent on how quickly a miner's computer can perform calculations as compared to those of other miners. Such users are described as miners because, in order to incentivise participants to engage in this process of validation, the system rewards the first to solve the puzzle with a preset quantity of new bitcoins. This did not require very much computational power in the beginning and anyone with a computer could mine bitcoin. However, as a result of the design of the bitcoin protocol, the level of difficulty increases with increased computational power participating in the network, and mining progressed from the use ordinary computers to dedicated ASIC (application-specific integrated circuit) chips that are designed to do nothing except mine for bitcoin.[11] Although computationally difficult to solve, the solutions are easily verifiable by other nodes, who may or may not be miners, on the network. Once verified, the transaction is added to the blockchain. This verification process requires a consensus of a majority of nodes in the network so that the likelihood of fraud is dramatically reduced.

A holder of bitcoins possesses a public bitcoin address and a private cryptographic key. The bitcoin address is often regarded as a serving a similar function to a bank account number. All that is needed to receive bitcoins is this public bitcoin address. Like a bank account, it is possible to have as many bitcoin addresses as one can be bothered to create. In order to transfer bitcoins out of the address, however, one requires both the address and the private cryptographic key. Whilst sometimes considered the equivalent of a password, the private cryptographic key is mathematically linked to the public address so that it is not possible to change the private key unlike a conventional password. One of the attractions of bitcoins is its relative anonymity compared with other payment systems. Although the first use of bitcoin in the real world was to purchase pizza,[12] in its early days, adoption was spurred

[11] Kevin Kelleher (22 December 2014), "The Gold Rush Days of Bitcoin Mining are Over, and Not Because of the Price", *Quartz* at https://qz.com/316898/the-gold-rush-days-of-bitcoin-mining-are-over-and-not-because-of-the-price/ (accessed 5 April 2017)

[12] Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (2015), 43-44.

by their use on an online black market website called Silk Road.[13] In order to ensure anonymity, "[c]redit cards and PayPal were not accepted. Bitcoins, a virtual currency, were".[14] "Thanks to Silk Road, Bitcoin was being regularly used for the first time as a medium of exchange for real, if illegal, things."[15] However, bitcoin addresses are not completely anonymous but only pseudo-anonymous. While the identity of the address holder is not known, all transactions related to the address are in fact transparent and tracked in the blockchain. With the appropriate information, including publicly available information, it is possible to track some bitcoin transactions. In the case of the mastermind behind Silk Road, Ross Ulbricht, who took to calling himself the Dread Pirate Roberts,[16] after a character from the movie *The Princess Bride*,[17] this allowed the FBI to identify and arrest him.[18] In Satoshi Nakamoto's white paper, in order to achieve greater privacy, it was recommended that "a new key pair should be used for each transaction to keep them from being linked to a common owner."[19] However, even such a strategy cannot promise complete anonymity. This is because, as previously held bitcoins have to be transferred to a new address, advanced data analytics will still enable one to link various addresses together and identify them as belonging to one user. It has been estimated that "almost 40% of users can be, to a large extent, recovered even when users adopt privacy measures recommended by Bitcoin."[20]

---

[13] Popper, *ibid*, 69-87. See also Joseph Goldstein (2 October 2013), "Arrest in U.S. Shuts Down a Black Market for Narcotics", *The New York Times*.

[14] Goldstein, *ibid*.

[15] Popper, n 12, 82.

[16] Popper, n 12, 118.

[17] *The Princess Bride*, Dir. Rob Reiner, 20th Century Fox, 1987.

[18] Andy Greenberg (29 January 2015), "Prosecutors Trace $13.4m in Bitcoins from the Silk Road to Ulbricht's Laptop", *Wired* at https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/ (accessed 5 April 2017).

[19] Satoshi Nakamoto, n 2, 6.

[20] Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun, "Evaluating User Privacy in Bitcoin" in Ahmad-Reza Sadeghi (ed), *Financial Cryptography and Data Security* (2013), 34.

This is a pre-print manuscript of a paper forthcoming in (2017) 9.2 Law, Innovation and Technology. Please refer to the journal at http://www.tandfonline.com/loi/rlit20 for the final version.

The open-source software for the implementation of this system of "electronic cash" was released by Satoshi Nakamoto on 3 January 2009.[21] As bitcoins gradually gained popularity,[22] bitcoin exchanges were established to enable individuals who wanted more bitcoins than they could mine to acquire them. An exchange rate of US$1 for 1,309.03 bitcoins was first established in October 2009. Prices rose rapidly and reached US$1,216 per bitcoin in late 2013.[23] Exponential growth in bitcoin prices initially created a network effect; there was an influx of both miners and investors. Bitcoin has proven attractive to speculative investors as supply is inherently limited (a limitation that was built into the system protocol by Satoshi Nakamoto) so that many expect its price to grow as the supply of new bitcoins dwindles. Although prices fell from their heady highs in 2013, usage of bitcoins rose.[24] In 2017, it briefly traded above both its 2013 peak and the price of an ounce of gold, at more than US$1,290 per bitcoin,[25] but its price remains prone to bouts of volatility.[26] Bitcoin has also spawned

[21] Joshua Davis (10 October 2011), "The Crypto-Currency Bitcoin and its mysterious inventor", *The New Yorker* at http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency (accessed 5 April 2017).

[22] See generally, Popper, n 12.

[23] Cade Metz (5 January 2016), "Thought Bitcoin was Dead? 2016 is the Year it Goes Big", *Wired* at https://www.wired.com/2016/01/thought-bitcoin-was-dead-2016-is-the-year-it-goes-big/ (accessed 5 April 2017).

[24] Metz, *ibid*.

[25] Rishi Iyengar (3 March 2017), "Bitcoin Price Exceeds Gold for First Time Ever", *CNN* at http://money.cnn.com/2017/03/03/investing/bitcoin-gold-price-value/ (accessed 5 April 2017). See also Robin Wigglesworth (3 March 2017), "Bitcoin Price Tops Gold for the First Time Ever", *Financial Times*. For a different, much earlier milestone, see Roger Ver (4 April 2017), "The Gold Rush Begins: The Day Bitcoin Topped the US Dollar", *Coindesk* at http://www.coindesk.com/the-gold-rush-begins-bitcoin-tops-the-dollar/ (accessed 5 April 2017).

[26] Joon Ian Wong (5 January 2017), "Bitcoin Lost $3 Billion in Market Value in 40 Minutes", *Quartz* at https://qz.com/878931/bitcoin-lost-3-billion-in-market-value-in-40-minutes/ (accessed 5 April 2017); Joon Ian Wong (10 February 2017), "A Chinese Clampdown Reveals a Fundamental Problem with the Bitcoin Markets", *Quartz* at https://qz.com/907629/bitcoin-yen-volumes-a-chinese-clampdown-reveals-a-fundamental-problem-with-the-bitcoin-markets/ (accessed 5 April 2017). See also Alex Lielacher (12 January 2017), "Bitcoin Volatility Reminds Investors About the Reality of Investing in Digital Currencies", *Bitcoin Magazine* at https://bitcoinmagazine.com/articles/bitcoin-volatility-reminds-investors-about-the-reality-of-investing-in-digital-currencies-1484253220/ (accessed 5 April 2017); Jonathan Garber (3

hundreds of alternative cryptocurrencies that are built upon the open-source code underpinning bitcoin.[27] These range from the cutesy dogecoin,[28] named after an Internet meme featuring a Shiba Inu dog accompanied by text in broken English, to the significantly more sinister darkcoin[29] and monero,[30] both designed to offer far greater anonymity than bitcoin. There are even some tentative suggestions by some government officials[31] and bodies[32] that official fiat cryptocurrencies may follow.

April 2017), "Bitcoin Spikes after Japan says it's a Legal Payment Method", *Business Insider Singapore* at http://www.businessinsider.sg/bitcoin-price-spikes-as-japan-recognizes-it-as-a-legal-payment-method-2017-4/?r=US&IR=T (accessed 5 April 2017); Willy Woo (5 January 2017), "Volatility and Liquidity: How Bitcoin Compares to its Crypto Competitors", *Coindesk* at http://www.coindesk.com/network-effects-volatility-liquidity-bitcoin-versus-payment-coins/ (accessed 5 April 2017).

[27] Nathaniel Popper (24 November 2013), "In Bitcoin's Orbit: Rival Virtual Currencies Vie for Acceptance", *The New York Times*. See also Quentin Hardy (6 March 2014), "Bitcoin is a Protocol. Bitcoin is a Brand.", *The New York Times*.

[28] Anthony Cuthbertson (8 December 2014), "Jackson Palmer: I Created $20m Dogecoin Phenomenon and all I have to Show for it is a Jar of Nutella", *International Business Times* at http://www.ibtimes.co.uk/jackson-palmer-year-dogecoin-jar-nutella-all-i-have-show-1478649 (accessed 5 April 2017).

[29] Andy Greenberg (21 May 2014), "Darkcoin, the Shadowy Cousin of Bitcoin, is Booming", *Wired* at https://www.wired.com/2014/05/darkcoin-is-booming/ (accessed 5 April 2017).

[30] Andy Greenberg (25 January 2017), "Monero, the Drug Dealer's Cryptocurrency of Choice, is on Fire", *Wired* at https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/ (accessed 5 April 2017).

[31] See, eg, Andrew G Haldane (18 September 2015), "How Low Can You Go?", Speech given at the Portadown Chamber of Commerce, Northern Ireland, available at http://www.bankofengland.co.uk/publications/Documents/speeches/2015/speech840.pdf (accessed 5 April 2017).

[32] John Barrdear and Michael Kumhof, "Staff Working Paper No. 605: The macroeconomics of Central Bank Issued Digital Currencies" (18 July 2016) at http://www.bankofengland.co.uk/research/Pages/workingpapers/2016/swp605.aspx (accessed 5 April 2017). See also Philip Stafford (17 June 2016), "Canada Experiments with Digital Dollar on Blockchain", *Financial Times*; Lulu Yilun Chen and Justina Lee (21 January 2016), "China Mulls Answer to Bitcoin with Digital Currency Study", *Bloomberg Business* at https://www.bloomberg.com/news/articles/2016-01-21/chinese-central-bank-studies-prospect-of-own-digital-currency (accessed 5 April 2017). The official statement of the People's Bank of China (in Chinese only) is available at http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3008070/index.html (accessed 5 April 2017).

This is a pre-print manuscript of a paper forthcoming in (2017) 9.2 Law, Innovation and Technology. Please refer to the journal at http://www.tandfonline.com/loi/rlit20 for the final version.

Whether or not fiat cryptocurrencies will eventually materialise or bitcoins or one of its derivatives achieves mainstream adoption,[33] it appears that bitcoins and its ilk are here to stay for the foreseeable future, even if only in the fringes.[34]

2. MONEY AS PROPERTY

It has been posited that "[c]oins, banknotes and bank money provide the core instances of money."[35] "Bank money" is the term economists used to describe balances held by customers in banking institutions.[36] This view is not, however, without controversy.[37] Bank money, or incorporeal money,[38] is as a matter of law, a chose in action, specifically a debt owing by the bank to its customer.[39] Whether choses in action are properly regarded as property is a subject of intense disagreement. Whilst a chose in action is often classified as a form of property, in so describing it, we are using "property" to mean something quite different from a classical *in rem* right. A right *in rem* is a right in or against a thing yet there doesn't appear to be any separate thing that is the subject of a debt other than the debt itself. Furthermore, a right cannot both be *in rem* and *in personam*. Incorporeal money in the form of a debt is unarguably *in personam* in nature. A classificatory scheme which purports to distinguish rights *in rem* from rights *in personam* but which then insists that rights *in personam* are themselves *in rem* rights is blatantly unsound. The problem is that, "property", as used by lawyers, is a dangerously slippery word and uncharacteristic of a profession that prides itself on precision. Birks famously distinguishes between the use of the label "property" to loosely mean "wealth" (which can include *in personam* and possibly other rights) and a stricter, more technical

[33] Nick Wingfield (30 October 2013), "Bitcoin Pursues the Mainstream", *The New York Times*.

[34] Cade Metz (12 November 2015), "Everyone Says Bitcoin is Back. But it Never Really Left", *Wired* at https://www.wired.com/2015/11/bitcoin-is-back-but-it-never-really-left/ (accessed 5 April 2017).

[35] David Fox, *Property Rights in Money* (2008), 16.

[36] See, eg, John Maynard Keynes, *A Treatise on Money* (1930), vol 1, 5-6.

[37] See, eg, Fox, n 35, 38-42.

[38] This is the expression favoured by Fox, *ibid*, 11.

[39] *Foley v Hill* (1848) 2 HLC 28, 9 ER 1002.

usage of the word.[40] According to Birks, in its more technical usage, property is distinguished from obligations by a bright line, of which the practical difference is borne of the question, "Against whom is the right exigible?" "A right *in rem* is a right the exigibility of which is defined by the location of a thing. A right *in personam* is defined by the location of the person."[41] Perhaps even more plainly, it is said that one of the hallmarks of a property right is its exigibility against strangers to its creation.[42] On this view, debts, including incorporeal money in the form of debts owed by banks, would not qualify as property at all.[43] An even stricter view would require the universally exigible right to be separable from a physical thing, preventing even intellectual property rights from qualifying as property.[44]

Whilst this insistence on separability may seem curious and somewhat fundamentalist, it does in fact serve a useful purpose. Such a strict usage of the word "property" would avoid the confusion stemming from a failure to distinguish between the different uses of the word. At the risk of oversimplification, some scholars argue that holders of *in personam* choses in action ought to be able to sue the world at large for unwarranted "interferences" because universal exigibility is a feature of property and a chose in action, even if *in personam*, is property. There are indeed tort actions that *appear* to protect against interferences with *in personam* choses in action. The economic tort of inducement of a breach of contract is the most obvious example. However, *in personam* choses in action were regarded as property well before[45] the modern tort of

[40] Peter Birks, 'Before We Begin: Five Keys to Land Law' in Susan Bright and John Dewar (eds), *Land Law: Themes and Perspectives* (1998) 457, 473.

[41] Birks, *ibid*.

[42] William Swadling, "Property: General Principles" in Andrew Burrows (ed), *English Private Law* (3rd ed, 2013), [4.03].

[43] Swadling, *ibid*, [4.20].

[44] Swadling, *ibid*. *Contra* William Swadling, "Property: General Principles" in Peter Birks (ed), *English Private Law*, vol 1 (2000), [4.52]. See also Simon Douglas and Ben McFarlane, "Defining Property Rights" in James Penner and Henry Smith (eds), *Philosophical Foundations of Property Law* (2013), 219 and Ben McFarlane, *The Structure of Property Law* (2008), 132-137.

[45] See, eg, William Blackstone, *Commentaries on the Laws of England Volume 2 Of the Rights of Things* (1765-1769), 442.

inducement of breach of contract evolved[46] out of the action for enticement of a servant founded upon the Statute of Labourers 1349 in the case of *Lumley v Gye*.[47] Furthermore, the tort of inducement of breach of contract is more appropriately regarded as a species of accessory liability[48] than as a property tort. It is more closely related to joint tortfeasance than conversion, trespass or any property tort. A narrow definition of "property" better enables us to see that *in personam* "not property" behaves very differently from *in rem* "property". However, it is possible to reach the same conclusion without taking such a narrow definition of "property". We could instead simply recognise that the appellation "property" does *not* carry with it any necessary indication of strict rights against third parties for interferences. It is of course possible for the law to develop such rights,[49] perhaps by further evolving the tort of inducement of breach of contract, some other economic tort or by adapting the tort of conversion, but it is important to recognise that such a development is neither necessary nor necessarily desirable.[50] Perhaps more to the point, such a development should not be dictated by whether or not a right attracted the label of "property".

A broader definition of "property" is preferable because the narrow definition obscures similarities in legal rules applicable to both transferable *in rem* rights and transferable *in personam* rights. The legal rules relating to competing claims to such assets, to employ a neutral term, including the general rule of *nemo dat quod non habet* and its various exceptions, are examples of such rules applicable to all legally transferable rights. Thus viewed, Birks' strict conception of "property" seems excessively narrow.[51] Rather than being symptomatic of laxity, the broader label of "property" refers to the law's recognition of and willingness to enforce a holder's rights to exclude others from a resource,[52] whether tangible or intangible, without necessarily

[46] See, generally, Hazel Carty, *An Analysis of the Economic Torts* (2nd ed, 2010), Chap 3.

[47] [1853] 2 E&B 216.

[48] See, eg, the inclusion of the tort in Paul Davies, *Accessory Liability* (2015), Chap 5.

[49] See, eg, the differences in opinion in *OBG Ltd v Allen* [2008] 1 AC 1.

[50] Amy Goymour, "Conversion of Contractual Rights" [2011] LMCLQ 67.

[51] Jim Harris, "Property – Rights *in Rem* or Wealth?" in Peter Birks and Arianna Pretto (eds), *Themes in Comparative Law: In Honour of Bernard Rudden* (2002), 51.

[52] Felix Cohen, "Dialogue on Private Property" (1954) 9 Rutgers L Rev 357, 370-371

providing any clues as to its exigibility. The role of the law of property is to identify the person holding this right to exclude. After all, "the word 'property' reflects its semantically correct root by identifying the condition of a particular resource as being 'proper' to a particular person."[53] One cannot assume that rights to exclude others from a resource may only be granted by the law through directly enforceable rights against an indefinite class of persons. While legal property rights to tangible things in common law systems take on this form, it is certainly not true of equitable property rights to tangible things, which take on a different, sometimes indirect, form. Suppose A declares that he holds his bicycle on trust for B. If C were to steal the bicycle from A, the law does not generally permit B to sue C directly.[54] Instead, B must sue A to direct him to sue C. B's equitable "property" behaves differently from a legal property in the bicycle. In this case, the right to exclude afforded by equity to B operates indirectly, through the medium of the trustee A. Where legal intangible property is concerned, it is a mistake to assume that a right confers a power to exclude only where it is enforceable against the world at large, for example, in the case of copyrights and patents.[55] Exigibility therefore is distinguishable from exclusivity. The law of property's concern over the power to exclude, in the context of choses in action, lies in the law's identification of the person who is able to provide relief to an obligor in law for the right of the obligee. This concern is the same whether we are concerned with choses in action that are *in personam* (such as debts) or *in rem* (such as patents). Suppose A is the holder of a patent for a widget. Suppose then that B pretends to be A and "licences" the patent to C, who proceeds to manufacture the widget. The "licence" is no defence to an action for patent infringement brought by A against C. This is because the law of property provides that only A is able to release C from his duty not to infringe the patent. This pattern is *exactly* the same where the subject-matter of the property is an *in personam* chose in action. Suppose A has been assigned a debt owing by D. Suppose then that B pretends to be A

[53] Kevin Gray and Susan Francis Gray, "The Idea of Property in Land" in Susan Bright and John Dewar (eds), *Land Law: Themes and Perspectives* (1998) 15, 15-16.

[54] *MCC Proceeds v Shearson Lehmann* [1998] 4 All ER 675. See also *Leigh and Sullivan Ltd v Aliakmon Shipping Co Ltd (The Aliakmon)* [1986] AC 785. Cf *Shell UK Ltd v Total UK Ltd* [2010] EWCA Civ 180, [2011] QB 86, noted Kelvin Low, "Equitable Title and Economic Loss" (2010) 126 LQR 507.

[55] Cf Swadling, n 44, [4.52].

and manages to convince D to "pay" him. Short of a provision to the contrary in the underlying contract, the "payment" by D to B would not absolve him of his duty to pay A because the law of property provides that only A may release him from his duty to make payment. Where there are multiple assignments, such as where the creditor first assigns to B and then purports to assign the same debt to C, the law of property tells us that it is not the timing of the assignment but the timing of each assignee's notification of the debtor D, that confers priority to the assignee.[56] On this view, the law of property does not tell us the content of the right (eg not to copy, not to manufacture, to make payment) nor its exigibility (eg against D alone, against the world at large). It merely tells us who among various competing parties may legitimately control those rights, whatever form their exigibility and content may take. Thus considered, incorporeal money in the form of bank money is properly regarded as property and this also leaves open the possibility that bitcoins and other cryptocurrencies may be treated as a species of property.

3. BITCOINS AS PROPERTY?

Since bitcoin is conceived of as a crypto*currency* and electronic *cash*, it seems sensible to begin a proprietary analysis by way of a comparison to more established forms of money.

3.1 ELIMINATING THE IMPOSSIBLE

It is obvious that bitcoins differ from corporeal money in the form of coins and banknotes since there is no *res* or tangible thing that comprises a bitcoin. If at all bitcoins can be considered property, it must be intangible. However, following the analysis above on the meaning of property, it would be a mistake to reason from an absence of a *res* to arrive at the conclusion that bitcoins are incapable of being owned as appears to have been done by the Tokyo District Court in a case[57] following the collapse

[56] The rule in *Dearle v Hall* (1828) 3 Russ 1.

[57] Kyodo (6 August 2015), "Bitcoins Lost in Mt Gox Debacle 'Not Subject to Ownership' Claims: Tokyo Court", *Japan Times* at http://www.japantimes.co.jp/news/2015/08/06/national/crime-legal/bitcoins-

of the bitcoin exchange Mt Gox.[58] Such a view of "property" is closely aligned with the strict Birksian view described above and stems from a development of the Roman law classification of legal rights into rights *in rem* and rights *in personam*. As explained by Fox in the context of conceptualising both corporeal and incorporeal money as property, three reasons compelled such a conclusion. "The first followed from the internal logic of the jurisits' institutional writings themselves. To ensure the absolute separation of the law of obligations from the law of things, the definition of things had to be narrowed so that it no longer included claims enforceable by action against a specific person."[59] "A second, related, reason [stemmed] from the need to find a defining feature of property rights as distinct from other rights which were generally enforceable against third parties."[60] "A third reason was the perceived need to maintain a legal concept of property distinct from a general economic notion of wealth."[61] Fox rightly notes that "[n]one of these reasons is compelling."[62] Furthermore, such a distinction also obscures the relationship across the categories of legal rules designed to allow the courts to identify the person(s) with the best claim to exercise exclusive control over a particular resource, whatever form that resource may take and conceals patterns that reveal themselves as obvious once our obsession with exigibility is abandoned. There is a distinction, after all, between seeing and observing.

Whilst it is clear that bitcoins, if they are to be conceived of as property, are intangible, it is also apparent that they are distinguishable from bank money or incorporeal money. Bank money, or incorporeal money, is derived from fiat currency in that it takes the form of a debt claim expressed in some form of fiat currency. The debtor or obligor is the bank with whom the customer has an account and this debtor/obligor is the trusted third party described in Satoshi Nakamoto's white paper.

---

lost-in-mt-gox-debacle-not-subject-to-ownership-claims-tokyo-court-rules/#.WOSioG997-0 (accessed 5 April 2017).

[58] See, generally, Leo Lewis (3 August 2015), "Japanese Police Hope to Shed Light on Bitcoin Exchange's Collapse", *Financial Times*.

[59] Fox, *supra* n 35, 36.

[60] Fox, *ibid*.

[61] Fox, *ibid*.

[62] Fox, *ibid*. See also 36-42.

As an electronic payment system conceived of as rendering such trusted third parties redundant, whatever form of intangible property it may be, bitcoins cannot take the form of a debt or an obligation for there is no one to take on the role of a debtor or obligor within the bitcoin network, at least not where the bitcoins are held directly as opposed to through a bitcoin exchange.[63] If bitcoins are neither tangible property nor debts or obligations, how then may they be conceived of as property?

3.2 DISMISSING THE INCONGRUOUS AND THE IMPRACTICAL

The next obvious suspect is the private cryptographic key that some commentators have associated with ownership. It has thus been suggested that "[t]here is no such thing as a Bitcoin. … If you own Bitcoin, what you actually own is the private cryptographic key to unlock a specific address."[64] The problem with this conceptualisation of bitcoin as property is that the private cryptographic key is nothing more than confidential information and the law does not generally countenance the idea of property in confidential information.[65] The reason that the law does not permit the ownership of pure information is not "because it is replicable or 'inexhaustible'".[66] Whilst it is true that "if you 'steal' the password for my phone, you have not removed it from me",[67] expressions in copyrighted works are likewise infinitely replicable and inexhaustible but for the legal constraints imposed by copyright law. Rather, this is because if anyone is to be given *exclusive* control over information, confidential or otherwise, then such control would serve as a grave impairment of the free flow of

[63] See below, text accompanying nn 154-165.

[64] Adrianne Jeffries (19 December 2013), "How to Steal Bitcoin in Three Easy Steps", *The Verge* at http://www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps (accessed 5 April 2017).

[65] See, generally, Tanya Aplin et al, *Gurry on Breach of Confidence: The Protection of Confidential Information* (2nd ed, 2012), 121-137. Cf *Veolia ES Nottinghamshire Ltd v Nottinghamshire County Council* [2010] EWCA Civ 1214, criticised by Tanya Aplin, "Confidential Information as Property?" (2013) 24 KLJ 172.

[66] Cf Tatiana Cutts and David Goldstone QC (14 June 2015), "Bitcoin Ownership and its Impact on Fungibility" *Coindesk* at http://www.coindesk.com/bitcoin-ownership-impact-fungibility/ (accessed 5 April 2017).

[67] Cutts and Goldstone, *ibid*.

information and the freedom of expression. Disastrous consequences would follow if the law recognised a right to exclusive control over even as discrete a piece of information as a private cryptographic key, e.g. 5KkKR3VAjjPbHPzi3pWEHVQWrVa3C4fwD4PjR9wWgSaV2D3kdmeM, if it subsequently turned out to be the answer to the Ultimate Question of Life, the Universe, and Everything. The action in breach of confidence, in contrast, provides only *limited* control to the person reposing confidence in another. The right to control the information through the action is not exigible against the world at large but only exercisable against a limited number of persons who acquire the information under certain circumstances.[68] Hence, it provides *limited* rather than *exclusive* control over the information and cannot properly be regarded as a form of property in information. While the exigibility of the cause of action is quite limited, the means of control proffered by the law over the persons affected is quite extensive. Persons subject to the right are legally bound from using or disclosing the information without authorisation.[69]

From the idea of conceptualising rights to bitcoins as rights to the private cryptographic key, we can derive two possible views as to how the private law ought to treat rights to bitcoin. First, it is possible to conclude that rights to bitcoins fall entirely outside the scope of the law of property, even as broadly conceived in this paper, and protection is limited to the law relating to confidential information. Secondly, it is possible to narrow the scope of control over the information that comprises the private cryptographic key so as to avoid the public policy concerns over propertising information. Thus, instead of granting broad control over use and dissemination, it is arguably possible to conceive of the right to the private cryptographic key as the right to use the key *to effect "transfers" out of its corresponding specific public bitcoin address*. So conceived, it is possible to avoid concerns over the possible impediment of the free flow of information and the freedom of expression. By narrowing the content of the right, it is possible to avoid these public policy concerns even if the right is regarded as universally exigible. The problem with this second view, as a matter of the law of property, is that

[68] See, Aplin, *Gurry on Breach of Confidence*, n 65, 241-300.

[69] See Aplin, *ibid*, 664-677.

even if it is regarded as providing *exclusive* but *narrow* control over the information comprising the private cryptographic key, *that* is not the right transferred when a holder transfers bitcoins to another holder. This is because when bitcoins are transferred from one public bitcoin address to another, the transferee acquires a separate private cryptographic key altogether. Thus, even on the broad view of property suggested, where the abstract right itself rather than information is treated as the resource, the role of the law of property in locating control over the right is absent since the right is never transferred.

So analysed, transfers of bitcoins appears analogous to the transfer of money between bank accounts rather than a normal conception of a transfer of property, such as occurs with a transfer of corporeal money. "The first and most obvious difference from a transfer of corporeal money is that the beneficiary does not obtain the same asset as previously belonged to the originator. It is not like a transfer of the very same coins or banknotes from the payor to the recipient, as happens when a person pays corporeal money."[70] Thus, "[t]he explanation of how property in incorporeal money is transferred has very little to do with the law governing the transfer of chattels by delivery."[71] In truth, there is no "transfer" as traditionally understood in the law of property: there is a transfer in value rather than a transfer in title.[72] Likewise, the transferee does not acquire the right to use the transferor's private cryptographic key to transfer bitcoins out of the transferor's public bitcoin address. Rather, the transferee acquires the right to use a different private cryptographic key to transfer bitcoins out of a different public bitcoin address. There are, however, differences between a transfer of money between bank accounts and a transfer of bitcoins so analysed. First, there is no agency relation involved in transfers of bitcoins as there is no trusted third party involved as obligor. Secondly, credit balance in a bank account can, as a chose in action, be truly transferred in the sense conceived of in the law of property even if no one ever does so. Choses in action that are not comprised in bank accounts are often assigned in this sense at a discount before maturity. It is not clear that, so analysed, the right to use

[70] Fox, n 35, [5.25].

[71] Fox, *ibid*, [5.03].

[72] Fox, *ibid*, [5.05].

the private cryptographic key to transfer bitcoins out of a specific public bitcoin address ought to be so transferable. Whereas the incongruity between the understanding of transfers between bank accounts by laypersons and the correct legal analysis may be justified by the need to accommodate the debtor-creditor relationship between bank and customer,[73] no such justification exists for a similar mismatch in lay understanding and legal analysis for transfers of bitcoin. There is a further drawback to this account. Because the right to bitcoins is conceived of in indirect terms through a right to one's private cryptographic key, the link between the value inherent in a bitcoin and the right conferred by the law becomes more tenuous. It is possible, after all, to hold the private cryptographic key to a public bitcoin address that "contains" zero bitcoins.

A further possibility that has been suggested is that the law of property is the wrong tool to encourage and support the further development and adoption of bitcoins. Thus, it has been suggested that:[74]

> [W]e must not assume that legal protections are necessary to drive a particular digital economy. Copyright law is the most obvious example of a tool that has fallen far behind in the search to secure sufficient protection to support industry growth. Access to online newspapers, music, audiobooks, images – the list goes on – is restricted not by the law of copyright, but by code.
>
> Bitcoin has built-in cryptographic protections, a plethora of offline storage options, and it seems increasingly likely that the transactional record provided by the blockchain will itself disincentivise abuse.

Such a legal position would be aligned with one conception of immutability that a not insignificant segment of cryptocurrency enthusiasts subscribe to.[75] The problems with this view, which would keep bitcoins and other cryptocurrencies essentially extra-legal as a matter of private law, are numerous. First, while bitcoin is often promoted on the

[73] *Foley v Hill*, n 39. See also, Benjamin Geva, "'Bank Money': The Rise, Fall, and Metamorphosis of the 'Transferable Deposit'" in David Fox and Wolfgang Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (2016), 359.

[74] Cutts and Goldstone, n 66.

[75] See below, text accompanying nn 102-109.

basis of its security, the cryptographic protocols of the blockchain only promise to prevent double-spending. They provide *zero* protection from other forms of fraud. When bitcoin devotees refer to bitcoin as being more secure than centralised systems, they are referring to system-wide security, not security for individual users. Users of the bitcoin network are vulnerable at several levels. Some of these vulnerabilities are theoretical but many have in fact been exploited in practice. At the personal level, a person's private cryptographic key can be "stolen". If it is stored electronically on his personal computer or mobile device, this "theft" can be achieved using malicious e-mail attachments or applications or by using keystroke logging devices or software to trace the private cryptographic key as it is typed in. Hacking is not only possible but regarded by some as commonplace. As the *Financial Times* reported, '[o]nline lists curated by bitcoin community members suggest bitcoin exchanges have been involved in up to 60 high-profile hacking incidents since the digital asset class was created in 2009. The true scale of the hacking problem, however, is hard to estimate.'[76] Even if the private cryptographic key is not stored electronically but offline, for example using a so-called paper wallet, access to the private cryptographic key will still allow a "thief" to make off with one's bitcoins, as happened to the CEO of a financial services company who left his account information in his car while having it valet parked.[77] These risks are exacerbated by the risk of loss of value through loss of the private key, which translates to a need to back it up. However, every additional backup, whether hot or cold, creates

[76] Izabella Kaminska (4 August 2016), "Bitcoin Bitfinex Exchange Hacked: the Unanswered Questions", *Financial Times*. See also Joon Ian Wong (4 August 2016), "Bitcoin Exchanges can't stop getting Hacked, no matter what Security System they Use", *Quartz* at https://qz.com/749789/bitcoin-exchanges-cant-stop-getting-hacked-no-matter-what-security-system-they-use/ (accessed 5 April 2017), Yuki Nakamura (18 August 2016), "The Wretched, Endless Cycle of Bitcoin Hacks", *Bloomberg* at https://www.bloomberg.com/news/articles/2016-08-17/the-wretched-endless-cycle-of-bitcoin-hacks (accessed 5 April 2017). For a comprehensive academic study of the risks of bitcoin exchanges, see Tyler Moore and Nicolas Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk" in Ahmad-Reza Sadeghi (ed), *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Revised Selected Papers, Lecture Notes in Computer Science, vol 7859* (2013), 25.

[77] Elliot Maras (11 November 2015), "Researcher Has Bitcoin Stolen off His Back in a Public Experiment", *Crypto Coins News* at https://www.cryptocoinsnews.com/researcher-bitcoin-stolen-off-back-public-experiment/ (accessed 5 April 2017).

another point of access to the private key by hackers or rogues. At the exchange level, security loopholes may allow hackers to gain access to an exchange's hot wallet. The most famous case of such a hack is that of Mt Gox, one of the earliest and biggest bitcoin exchanges where US$460 million worth of bitcoins were apparently stolen by hackers.[78] More recently, Cryptsy, a multi-crytocurrency exchange, claimed that about US$9 million worth of bitcoins and litecoins were stolen through a hack.[79] There are also security flaws at the network level though the threat here has remained entirely theoretical. Technically, if a person or more likely group of persons gains control of more than 50% of the total network hash power of the bitcoin network, they can invalidate transactions and/or double spend bitcoins from their own bitcoin addresses. Such an attack is unlikely to occur for a number of reasons. First, it is extremely expensive to amass sufficient computing power to launch such an attack. Secondly, such an attack will lead to widespread reluctance to accept bitcoins as payment, causing its value to plummet; a counterproductive effect for persons controlling sufficient nodes to launch such an attack as they are likely to hold a lot of bitcoins.[80]

The second problem with subscribing to absolute immutability is that it is probably inconsistent with the views of a majority of cryptocurrency investors, as can be seen in majority approval of the ethereum hard fork following the DAO attack.[81] Furthermore, while it is true that "the ability to exercise practical exclusive control over some asset must trump the ability to pay lawyers to chase it around the globe",[82] the two methods of protecting value, legal and extralegal, are not mutually exclusive. The same argument could be made for almost all forms of property – it is, for example,

[78] Robert McMillan (3 March 2014), "The Inside Story of Mt Gox, Bitcoin's $460 Million Disaster", *Wired* at https://www.wired.com/2014/03/bitcoin-exchange/ (accessed 5 April 2017).

[79] Stan Higgins (15 January 2016), "Cryptsy Threatens Bankruptcy, Claims Millions Lost in Bitcoin Heist", *Coindesk* at http://www.coindesk.com/cryptsy-bankruptcy-millions-bitcoin-stolen/ (accessed 5 April 2017).

[80] See Joshua A Kroll, Ian C Davey and Edward W Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries" *The Twelfth Workshop on the Economics of Information Security* (2013), 11-12.

[81] See below, text accompanying nn 102-111.

[82] Cutts and Goldstone, n 66.

cheaper to lock one's car than track it down after it is stolen and sue the thief – but they remain protected by the law.

The other justification against the propertisation of bitcoins is that for bitcoin to serve its purpose as a crypto*currency*, it is important for the law to encourage economic fungibility. Cutts and Goldstone therefore argue that "[t]here is … a good policy reason for the conclusion that one cannot, in a private law sense, 'own' bitcoin."[83] At the very least, they suggest that "[i]f we *do* apply property protections to bitcoin, it will be necessary to embrace wholeheartedly the exception for money media."[84] The necessity of negotiability to promote economic fungibility in order to ensure the proper functioning of currency has been doubted[85] but even if it is correct, there is a marked difference in legal consequences between a regime whereby property rights are withheld and one in which property rights are enforced but subject to a wide negotiability exception. As Cutts and Goldstone acknowledge, negotiability serves as an exception, admittedly a wide one. The general rule remains that of *nemo dat quod non habet*. It is simply not the case that every recipient of bitcoin will satisfy the requirements of being a bona fide purchaser for value. The recipient may be a volunteer or may not have given value. The recipient may also be purchasing bitcoins as a specific good or commodity,[86] as may arguably be the case where speculators purchase bitcoins expecting their value to appreciate.[87] A legal regime withholding property protection will accordingly exceed what the law presently regards as the appropriate balance between the rights of the former owner and those of the recipient in order to promote economic fungibility. While this is not fundamentally impossible, Cutts and Goldstone offer no justification for tipping the scales in this fashion. There is also the not insignificant problem that bitcoins, despite its apparent popularity, is not really being used as a medium of exchange to purchase goods and services as such.[88]

3.3 PONDERING THE IMPROBABLE

[83] Cutts and Goldstone, *ibid*.

[84] Cutts and Goldstone, *ibid*.

[85] JS Rogers, "Negotiability, Property and Identity" (1990) 12 Cardozo L Rev 471. Cf Fox, n 35, 49-67.

[86] Cf *Moss v Hancock* [1899] 2 QB 111.

[87] Metz, n 23.

[88] See below, text accompanying nn 127-130.

This leaves the final possibility which does not appear to have been considered. It is posited that the right may well be conceived of, to use language familiar to lawyers, as the right to have one's public bitcoin address appear as the last entry in the blockchain in relation to a particular bitcoin. The failure to contemplate this possibility may well stem from the fact that this departs from the normal function of a register (or ledger) in the law. Registration systems typically serve as *records* of rights. They do *not* normally represent the rights themselves. Thus, in the context of carbon credits for which an electronic register exists, it is simply wrong to claim that a carbon credit "exists only in electronic form."[89] It is the inconclusive *record* that exists in electronic form. Carbon credits are intangible and have no form whatsoever. Registers, as distinct from the rights they record, are heterogenous and function differently depending on design. Some registration systems provide prima facie evidence of title such as the case of shares,[90] patents,[91] and registered designs.[92] Some registration systems, such as that for trade marks, do not purport to provide any indication as to title at all, whether prima facie or otherwise.[93] So far as bank ledgers go, "in the absence of fraud, the customer is not precluded by the bank statement or the pass-book from disputing an error or an incorrect debit made by the bank or from insisting on its correction."[94] At the other extreme, registration of a fee simple title to land provides far greater protection than prima facie evidence of title, going so far as to validate an otherwise void transfer. Section 58(1) of the English Land Registration Act 2002 provides: "If, on the entry of a person as the proprietor of a legal estate, the legal estate would not otherwise be vested in him, it shall be deemed to be vested in him as a result of the registration." The entry of a notice on the register of an equitable interest in land behaves differently again, providing priority without validating invalid transfers. Section 32(3) of the English Land Registration Act 2002 provides: "The fact that an interest is the subject of a notice does

[89] *Armstrong DLW GmbH v Winnington Networks Ltd* [2013] Ch 156, [49], criticised by Kelvin FK Low and Jolene Lin, "Carbon Credits as EU Like It: Property, Immunity, TragiCO_2medy?" (2015) 27 *Journal of Environmental Law* 377.

[90] s127 Companies Act 2006.

[91] s 32(9) Patents Act 1977.

[92] s 17(8) Registered Designs Act 1949.

[93] Trade Marks Act 1994.

[94] E P Ellinger, E Lomnicka and C V M Hare, *Ellinger's Modern Banking Law* (5th ed, 2011), 236.

not necessarily mean that the interest is valid, but does mean that the priority of the interest, if valid, is protected for the purposes of sections 29 and 30."

The proposed analysis – that holders of bitcoins have the legal right to have their bitcoins, or more accurately their unspent transaction output or UTXO, locked to their chosen public bitcoin address on the blockchain – conceives of the right as being inseparable from the final entry in the register, here the blockchain. Such a right provides *exclusive* control to bitcoin holders in the form of universal exigibility and can be conceived of as involving a true property transfer when one user transfers bitcoin from his public bitcoin address to another user's public bitcoin address. Such an analysis allows for the legal protection of the value of bitcoins for holders while having a negligible effect on the liberties of others, which is a key consideration in formulating universally exigible rights. Where property rights take the form of universally exigible rights, the law is necessarily engaged in a delicate balancing exercise. Allocating more universally exigible rights to a property owner necessarily impinges on the liberties of everyone else. Hence, there is no fixed immutable list of rights that attach to property.[95] For example, unlike rights to land, for which the tort of private nuisance exists, there is generally no legal protection for more ephemeral and intangible interferences with the use of goods. Thus, to say that the law of property in the sense of *in rem* rights provides A with exclusive rights to a thing barely begins to tell us anything of value for it does not elucidate what those rights entail. The torts protecting property rights to goods principally protect rights to possession. Thus, if B creates a din so that A cannot hear the ringing of his mobile phone, B commits no tort and A has no legal claim against him. Even where the right is one to land, the law affords no protection from visual trespass.[96] Thus, in the context of *in rem* rights, or property rights relating to external things, the law appears to regard possessory rights as both more valuable to the property owner and less invasive of the personal liberties of everyone else. The link between the value inherent in the bitcoin is also more direct on this analysis than in the formulation involving a right to the private cryptographic key. Whilst this analysis involves the

[95] Craig Rotherham, "Property and Justice" in Matthew H Kramer (ed), *Rights, Wrongs and Responsibilities* (2001), 148.

[96] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.

conceptualisation of a register behaving in a very different and unusual manner, it has been suggested by a famous (admittedly fictional) sleuth that "when you have eliminated the impossible, whatever remains, *however improbable*, must be the truth".[97] [Emphasis in original]

4. LIMITS TO LEGAL RIGHTS

While we maintain the view that blockchain 'immutability' as a feature of bitcoins and other cryptocurrencies ought not to prevent holders of the same from having private law rights to them, it would undoubtedly affect the remedies that courts can order. It is also important to consider the very special scenario of forks in the blockchain.

4.1 REMEDIES IN THE FACE OF IMMUTABILITY

Concluding that legal rights can exist leads inevitably to the question of how those rights may be protected through remedies enforced by the legal system. In this respect, one of the key features of bitcoins – immutability[98] – will necessarily have an impact on the remedies that are available to a claimant at law. First, though, we need to consider the concept of immutability of the blockchain. There is no reference to immutability in Satoshi Nakamoto's white paper that introduced bitcoin to the world. The blockchain is not referred to as immutable but rather as a record that is "computationally impractical for an attacker to *change* if honest nodes control a majority of CPU power."[99] [Emphasis added.] Rather than consider immutability in the abstract, it is important to understand immutability from the perspective of the users of bitcoins. According to Antony Lewis, who runs the website *Bits on Blocks*:[100]

> **Immutability is relative.** For example if I send an email to a large list of

[97] Arthur Conan Doyle, *The Sign of Four* (London: Specer Blackett, 1890), 93.

[98] Mengerian (14 March 2017), "Two Theories of Bitcoin", *Medium* at https://medium.com/@Mengerian/two-theories-of-bitcoin-f4da84468a7a (accessed 5 April 2017).

[99] Satoshi Nakamoto, n 2, 8.

[100] Anthony Lewis (29 February 2016), "A Gentle Introduction to Immutability of Blockchains", *Bits on Blocks* at https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/ (accessed 5 April 2017).

> friends, that data is pretty immutable from my perspective. To change it, I'd have to persuade my friends each to delete the email (or persuade Gmail and the people running all the mailservers of my friends). From my perspective, and with the control I have, that email is immutable – I can't unsend or revoke it without collaboration and risk of detection. [Emphasis in original]

It has already been demonstrated that whilst the bitcoin network is, as a whole, more robust than a centralised one, individual users may nevertheless have their private keys "stolen" and thus lose their bitcoins to hackers and other rogues.[101] It is difficult to imagine that a sizable number of the bitcoin community would take the view that such transactions should be practically irreversible.

The most hardcore adherents to immutability that we have seen to date are the backers of a cryptocurrency called ethereum classic, which was created following the infamous hack of a curious 'fund' called the DAO (or Decentralized Autonomous Organization). The DAO was set up as an investment fund which would allow all the investors to vote on the investments that it would make (as opposed to leaving that decision to fund managers).[102] It attracted more than US$168m worth of a cryptocurrency called ether, based on the ethereum network.[103] Unfortunately, on 17 June 2016, a hacker managed to siphon off some US$50m worth of the invested ether.[104] The hack severely tested the concept of immutability of the ethereum blockchain. The core developers of ethereum eventually decided on a hard fork of the ledger, in effect a sort of reset that rolled back the entire ethereum network to its state before the hack.[105]

---

[101] See above, text accompanying nn 75-80.

[102] Cade Metz (6 June 2016), "The Biggest Crowdfunding Project Ever – the DAO – is Kind of a Mess", *Wired* at http://www.wired.com/2016/06/biggest-crowdfunding-project-ever-dao-mess/ (accessed 5 April 2017).

[103] Nathaniel Popper (27 March 2016), "Ethereum, a Virtual Currency, Enables Transactions that Rival Bitcoin's", *The New York Times*.

[104] Klint Finley (18 June 2016), "A $50 Million Hack Just Showed that the DAO was all too Human", *Wired* at http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ (accessed 5 April 2017).

[105] Joon Ian Wong and Ian Kar (18 July 2016), "Everything You Need to Know about the Ethereum 'Hard Fork'", *Quartz* at http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/

The hard fork was approved by a majority of the ethereum network[106] and this in effect created two versions of the ethereum ledger. The original intent of the developers (and the majority voting for the hard fork) was for the compromised ledger to wither away. However, the original compromised ledger refused to go away.[107] The survival of this zombie chain that refuses to die, now styled as ethereum classic (ETC) to distinguish it from the hard forked ethereum (ETH), which is sometimes also called ethereum one,[108] demonstrates that there is a significant segment of the cryptocurrency community who "would like to see a strict adherence to the original concept of code as law."[109]

Even so, a few observations are in order. First, the hard fork proposed and effected by the developers of ethereum in effect rolled back the ethereum blockchain to its state before the DAO hack. A court of law could not order such a remedy. Unlike a centralised register, which a court can order the registrar to rectify,[110] it is simply impractical to order the rectification of a decentralised register such as the bitcoin blockchain. The blockchain is stored across the network on thousands of computers spread across the world. It would be well-nigh impossible to enforce such an order against all such users. It is far simpler to order the person who effected or received the unauthorised transfer to retransfer a similar quantity of cryptocurrency, or their value

---

(accessed 5 April 2017). For a more detailed understanding of forks, see below, text accompanying nn 131-153.

[106] Andrew Quentson (8 July 2016), "Ethereum Reaches Unanimous Agreement to Hardfork", *Crypto Coins News* at https://www.cryptocoinsnews.com/ethereum-reaches-unanimous-agreement-hardfork/ (accessed 5 April 2017).

[107] Aaron van Wirdum (20 July 2016), "Rejecting Today's Hard Fork, the Ethereum Classic Project Continues on the Original Chain: Here's Why", *Bitcoin Magazine* at https://bitcoinmagazine.com/articles/rejecting-today-s-hard-fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808 (accessed 5 April 2017).

[108] Aaron van Wirdum (30 July 2016), "How the Great Schism Can End Well for Ethereum One", *Bitcoin Magazine* at https://bitcoinmagazine.com/articles/how-the-great-schism-can-end-well-for-ethereum-one-part-of-1469895898/ (accessed 5 April 2017).

[109] Kyle Torpey (5 August 2016), "Ethereum Experts Debate Merits of Two Ethereum Chains", *Bitcoin Magazine* at https://bitcoinmagazine.com/articles/ethereum-experts-debate-merits-of-two-ethereum-chains-1470432064 (accessed 5 April 2017).

[110] See, eg, s 20 of the English Land Registration Act 2002. See also s 21 of the same Act.

in fiat currency, to the rightful holder. Unlike the hard fork effected for ethereum, this does not entail rewriting transaction history as much as it merely adds a new transaction (if effected by payment in the relevant cryptocurrency) to the blockchain. If compensation is ordered in fiat currency, the blockchain is completely unaffected. As such, it is much less controversial than the hard fork effected in ethereum inasmuch as records are not rewritten. Secondly, it is notable that, despite the controversy the hard fork entailed, the majority of the ethereum community agreed to "to change ethereum's code to get the funds back to investors – and away from the attacker."[111] Thirdly, it is entirely possible that some of the minority who disagreed with the hard fork and ended up supporting the creation of the rival ethereum classic blockchain took the view that the hack was entirely permitted by the terms of the agreement between the participants of the DAO. After all, the founders of the DAO set out a term not unlike a standard "entire contracts clause"[112] on its website:[113]

> The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or

[111] Alyssa Hertig (28 July 2016), "Ethereum's Two Ethereums Explained", *Coindesk* at http://www.coindesk.com/ethereum-classic-explained-blockchain/ (accessed 5 April 2017).

[112] For a full explanation of the complexities surrounding the law relating to such clauses, see Kim Lewison, *The Interpretation of Contracts* (6th Ed, 2015), 135-139; Gerard McMeel, *The Construction of Contracts: Interpretation, Implication and Rectification* (2nd Ed, 2011), 687-734. See also David McLauchlan, "The Entire Agreement Clause: Conclusive or a Question of Weight?" (2012) 128 LQR 521; Lawrence Jacobson & Simon Mills, "Entire Agreement and Non-Reliance Clauses" (2001) 22 *Company Lawyer* 189; Alan Berg, "Thrashing Through the Undergrowth" (2006) 122 LQR 354; Alexander Trukhtanov, "Exclusion of Liability for Per-Contractual Misrepresentation: A Setback" (2011) 127 LQR 345; Matthew Barber, "The Limits of Entire Agreement Clauses" [2012] JBL 486.

[113] Although the terms have now been deleted from the DAO website, they can be found on Reddit: https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/d4cy4v0/ (accessed 5 April 2017).

> modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation.

As at least one commentator has pointed out, it is just about plausible to take the view that "according to the DAO's own legal contract, there is no such thing as theft and the intent is completely unimportant—the only important and relevant thing are the smart contracts themselves. Consequently, there is no real legal difference between a feature and an exploit. It is all a matter of perspective."[114] Whether this view is correct is beside the point for our purposes – it is probably wrong. While the hackers of the DAO had relied on weaknesses in the code of the DAO, which contained the abovementioned arguably legally effective clause, most hackers will not be able to point to similar provisions to justify their actions. Finally, it is not obvious that all the supporters of ethereum classic have done so as a matter of principle. One of the problems with permanent forks in the blockchain is that, under the right circumstances, they effectively give users who are willing to support both blockchains "free money".[115] It is entirely possible that many backers of ethereum classic were simply attracted to this "free money" and did not support it for ideological reasons.

Consequently, it is suggested that whilst immutability and the distributed nature of the bitcoin blockchain will prevent courts from ordering a rectification of the blockchain, it will not prevent courts from ordering parties who have illegitimately interfered with the rights of holders of bitcoins or other cryptocurrencies to pay such holders damages, either expressed in the relevant cryptocurrency or in the value of the same in fiat currency. Whether or not a court will make an order expressed in cryptocurrency will be dependent on the particular jurisdictions laws on the availability

[114] Joel Dietz (18 July 2016), "DAOs, Hacks and the Law", *Medium* at https://medium.com/@Swarm/daos-hacks-and-the-law-eb6a33808e3e (accessed 5 April 2017).

[115] See below, text accompanying nn 149-153.

of judgments in foreign currency[116] as well as whether or not that jurisdiction accepts cryptocurrencies as a form of foreign currency. In the latter respect, many of the decisions as to whether bitcoins are a currency or currency-like are unlikely to be helpful. First, they are not entirely consistent.[117] Secondly, they are almost always concerned with the meaning of currency in a particular statutory context, some of which may be wider than the ordinary sense of the word.[118] It is notable that in some of these cases, there is a concern to ensure that bitcoins cannot be used to evade rules regulating the transmission of moneys but a sensible inclusion for regulatory purposes does not always translate into the same treatment for other purposes. In this respect, it is pertinent to observe the ineptitude of the media covering cryptocurrencies as to precise legal terminology, thus perhaps breeding over-optimism among investors. Various recent news reports suggested that Japan has come to recognize "Bitcoin and other cryptocurrencies as legal tender",[119] causing a spike in the value of bitcoins.[120] However, more careful press reports suggest that "[t]he new law defines Bitcoin and other virtual currency as a form of payment method, not a legally-recognized

[116] For claims in debt, see Charles Proctor, *Mann on the Legal Aspect of Money* (7th ed, 2012), [8.03]-[8.18]. In particular, note the very different approaches of the US and the English courts. For claims in damages for torts, which are probably more relevant for our purposes, see Michael Howard, John Knott and John Kimbell, *Foreign Currency: Claims, Judgments and Damages* (2016), 128-146, but only in relation to English law. The key English cases are *Miliangos v George Frank (Textiles) Ltd* [1976] AC 443 and *Owners of the Eleftherotria v Owners of the Despina R* [1979] AC 685.

[117] See, eg, *Skatterverket v David Hedqvist* (C-264/14), 22 October 2015; *United States v 50.44 Bitcoins*, 2016 WL 3049166 (D Md 2016); *United States v Murgio*, 2016 WL 5107128 (SD NY 2016); *US v Faiella*, 39 F Supp 3d 544 (SD NY 2014); *contra Florida v Espinoza*, No F14-293 (Fla Cir Ct 22 July 2016).

[118] In this respect, *Skatterverket v David Hedqvist* (C-264/14), 22 October 2015 is particularly apposite. See the opinion of the European Court of Justice's Advocate General Juliane Kokott in the same case, 16 July 2015, [24]-[45].

[119] Nathan Reiff (3 April 2017), "Japan Finally Recognizes Bitcoin After Long Battle", *Investopedia* at http://www.investopedia.com/news/japan-finally-recognizes-bitcoin-after-long-battle/ (accessed 5 April 2017). See also Gautham (2 April 2017), "Japan Officially Recognises Bitcoin as Currency Starting April 2017", *NewsBTC* at http://www.newsbtc.com/2017/04/02/japan-officially-recognises-bitcoin-currency-starting-april-2017/ (accessed 5 April 2017).

[120] Joseph Young (3 April 2017), "Bitcoin Price Hits $1,130, Japan Legalizes Bitcoin, Scaling Progress", *The CoinTelegraph* at https://cointelegraph.com/news/bitcoin-price-hits-1130-japan-legalizes-bitcoin-scaling-progress (accessed 5 April 2017). Cf Garber, n 26.

currency."[121] Acknowledging that something can be used as a means of payment[122] and seeking to regulate it does not make the means of payment legal tender.[123] Thirdly, despite some differences in implementation, bitcoin and other cryptocurrencies appear to fit the description of alternative money, which are currencies that "challenge … the monopoly exercised by governments in creating official *fiat* money".[124] For remedial purposes, "under English law, alternative money will be regarded not as money but as a commodity,"[125] so that damages will be assessed in accordance with normal principles. If this is correct, this exposes bitcoin holders to fluctuations in prices between the date in which their rights are interfered with and the date on which judgment is satisfied although this is ameliorated to the extent that a jurisdiction does not inflexibly stick to the so-called "breach date rule".[126] Fourthly, despite all the attention, bitcoin really isn't very much used. As the *Financial Times* reported, "the sum of [daily] bitcoin transactions rounds to zero."[127] Furthermore, according to data assembled by Chainanlysis for *New York Times*, out of all the transactions involving bitcoins, "most of the transactions come from exchanges … where people speculate on the value of the

[121] Luke Parker (1 April 2017), "Bitcoin Regulation Overhaul in Japan", *Brave New Coin* at https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan/ (accessed 5 April 2017).

[122] This recent Japanese development mirrors somewhat the immediate aftermath of the shutting down of the Silk Road. FBI Special Agent Christopher Tarbell described bitcoins as follows in the criminal complaint against Ross Ulbricht: "Bitcoins are not illegal in and of themselves and have known legitimate uses. However, bitcoins are also known to be used with cybercriminals for money-laundering purposes, given the ease with which they can be used to move money anonymously." (at para 21(b)(v)) This brief statement, which is unexceptional as a matter of legal analysis, was latched onto by investors searching for hope in the aftermath of the destruction of bitcoin's then largest market: see Robert McMillan (2 February 2013), "Bitcoin Values Plummet $500m, then Recover, after Silk Road Bust", *Wired* at https://www.wired.com/2013/10/bitcoin-market-drops-600-million-on-silk-road-bust/ (accessed 5 April 2017).

[123] For a definition of tender, see Fox, n 35, 28.

[124] Howard, Knott and Kimbell, n 116, 334.

[125] Howard, Knott and Kimbell, *ibid*, 338.

[126] Andrew Dyson and Adam Kramer, "There is no "Breach Date Rule": Mitigation, Difference in Value and Date of Assessment" (2014), 130 LQR 259. See also Michael Bridge, "Markets and Damages in Sale of Goods Cases" (2016) 132 LQR 405.

[127] Dan McCrum (3 January 2017), "Bitcoin Passes $1,000 but Only Number that Matters is Zero", *Financial Times*.

currency. People using Bitcoin to buy or sell products or services are a small proportion of all transactions."[128] In this respect, it is notable that the services most likely to see payment in bitcoin include bitcoin mining, bitcoin mixing,[129] and purchases on dark markets.[130] Accordingly, it seems highly improbable that the courts will treat bitcoins or other cryptocurrencies in the same way as they would foreign *fiat* currencies for remedial purposes.

4.2 A FORK IN THE BLOCKCHAIN

In his poem, "The Road Not Taken",[131] regarded by some as the most misread poem in America,[132] the celebrated American poet Robert Frost, through the clever use of language, pulled off a remarkable conjuring trick. Written for his friend Edward Thomas,[133] it is often considered by many "to be a paean to triumphant self-assertion".[134] However, the poem "both is and isn't about individualism, and it both is and isn't about rationalization."[135] "Part of its trick", it has been remarked, "is that it enacts what it has previously claimed is impossible: the traveling of two roads at once."[136] "It is a poem about the necessity of choosing that somehow, like its author, never makes a choice itself—that instead repeatedly returns us to the same enigmatic,

---

[128] Nathaniel Popper (29 June 2016), "How China Took Center Stage in Bitcoin's Civil War", *The New York Times*.

[129] This is a service akin to money laundering that involves mixing Bitcoin transactions so as to obscure the source of the transactions.

[130] Online black markets, the most famous of which was the Silk Road. Whilst the Silk Road has been shut down, other dark markets have taken its place.

[131] Robert Frost, *Mountain Interval* (1916), 9.

[132] David Orr, *The Road Not Taken: Finding America in the Poem Everyone Loves and Almost Everyone Gets Wrong* (2015).

[133] Matthew Hollis (29 July 2011), "Edward Thomas, Robert Frost and the Road to War", *The Guardian* at https://www.theguardian.com/books/2011/jul/29/robert-frost-edward-thomas-poetry (accessed 5 April 2017).

[134] Orr, n 132, 8.

[135] Orr, *ibid*, 12.

[136] Katherine Robinson, "Robert Frost: 'The Road Not Taken'", *Poetry Foundation* at https://www.poetryfoundation.org/resources/learning/core-poems/detail/44272#guide (accessed 5 April 2017).

leaf-shadowed crossroads.[137] Whilst the ambiguity inherent in natural language which permits the trick pulled off by Frost is not permitted by code as a programming language,[138] the blockchain that undergirds bitcoin and other cryptocurrencies do permit a similar trick through the possibility of maintaining two blockchains at once when a fork occurs.

Before an explanation of blockchain forks can be given, it is useful to recall that the bitcoin blockchain conceives of a distributed, as opposed to a centralised, ledger. As a record keeping system, decentralised systems such as that envisaged by bitcoin, inherently permit the possibility, impossible in the case of a single centralised ledger,[139] that different participants in the network may maintain a slightly different record. The bitcoin ledgers, which should in theory be identical, sit on nodes connected to the bitcoin network. Originally, to be regarded as a full node, a computer had to run a client (ie software) which must download every transaction that has ever taken place on the bitcoin network since Satoshi Nakamoto mined the first 50 bitcoins on 3 January 2009,[140] all new transactions and block headers, as well as store information about every unspent transaction output until it is spent. For most users, this was extremely inefficient since they would be required to store the entire blockchain, which is a huge and ever-growing file,[141] so it was common for users to be advised to run a lightweight client instead. Full nodes need not perform any mining service[142] though all miners (or mining pools) must run at least one full node. Although they do not, unless they are also miners, add new blocks to the blockchain, full nodes formed the backbone of the bitcoin network, by both transmitting and validating transaction information. Although more recent reference clients permit full validating nodes to prune the blockchain and store only information relating to unspent transaction output, many users still prefer not to

[137] Orr, n 132, 12.

[138] RLG (31 July 2012), "Why Language Isn't Computer Code", *The Economist*.

[139] This is not to say that the central ledger is accurate or must be so regarded.

[140] Wallace, n 3.

[141] 109,509 megabytes as at 4 April 2017, according to https://blockchain.info/charts/blocks-size (accessed 5 April 2017).

[142] Cf Ben (27 December 2015), "What is a 'Full-Node'?", *Medium* at https://medium.com/@shibuyashadows/what-is-a-full-node-a64bd71b5d0c (accessed 5 April 2017).

operate full nodes.[143] Even if a user runs a full node, he may not be using the most recent reference client. The existence of different clients that are used by different users on the network creates potential compatibility issues, leading to the possibility of the blockchain forking.

Forks can be broadly divided into four categories, depending on compatibility and whether they occur by design or by accident.[144] In so categorising them, we are treating as irrelevant forks in the blockchain that arise purely from the distributed nature of the blockchain. Such forks occur anytime two different miners successfully mine a block at nearly the same time are simply a byproduct of the distributed nature of the ledger. The blockchain protocol resolves such forks through the adoption of the rule that "nodes always work on the longest version of the blockchain there is".[145] Accordingly, the first of these two blockchains to have a subsequent block added to it will be adopted by the network whereas the other blockchain will be abandoned, or in the language of the bitcoin community, orphaned. The forks in the blockchain that we are concerned with arise otherwise than purely from the distributed nature of the network. These forks are usually, but not always, introduced by software upgrades. Indeed, the use of the word "fork" to describe such incidences probably stems from its use as a technical term to describe software updates in open source projects. A hard fork to the blockchain is introduced by a software upgrade that introduces a new rule that is incompatible with that of older software whereas a soft fork is instituted by a new rule that is backward compatible. Put in terms of transaction validity, software upgrades introducing hard forks will regard as valid some transactions previously considered invalid whereas those introducing soft forks will treat as invalid some

[143] Luke Parker (16 June 2015), "The Decline in Bitcoin Full Nodes", *Brave New Coin* at https://bravenewcoin.com/news/the-decline-in-bitcoins-full-nodes/ (accessed 5 April 2017), Daniel Dawrey (9 May 2014), "What are Bitcoin Nodes and Why do We Need Them?", *Coindesk* at http://www.coindesk.com/bitcoin-nodes-need/ (accessed 5 April 2017).

[144] Peter Smith and Kristov Atlas (26 February 2016), "A Brief History of Bitcoin Forks", *Blockchain Blog* at https://blog.blockchain.com/2016/02/26/a-brief-history-of-bitcoin-forks/ (accessed 5 April 2017). See also Amy Castor (27 March 2017), "A Short Guide to Bitcoin Forks", *Coindesk* at http://www.coindesk.com/short-guide-bitcoin-forks-explained/ (accessed 5 April 2017).

[145] Briefing (31 October 2015), "The Great Chain of Being Sure about Things", *The Economist*.

transactions that would previously be regarded as valid. A soft fork will only be effective if it is supported by a majority of the hash (or mining) power in the network or else it will become the shortest chain and be orphaned by the network. Forks of both varieties may arise by conscious design or by accident. The most famous fork experienced by the bitcoin network, in March 2013, was wholly unintended. On 11 March 2013, at about 23:30 GMT, bitcoin users first noticed "one of the most serious hiccups that we have seen [since the network came into being]. Starting from block 225430, the blockchain literally split into two, with one half of the network adding blocks to one version of the chain, and the other half adding to the other. For the next six hours, there were effectively two Bitcoin networks operating at the same time, each with its own version of the transaction history. The split lasted for 24 blocks or 6 hours, finally resolving itself when one version of the chain conclusively pulled ahead of the other at block 225454, leaving the other chain largely abandoned".[146] Today, this fork has been overshadowed by the ethereum hard fork, which was deliberate, following the DAO hack.[147] Although such a result has been described as "the worst case scenario",[148] a significant group of users of ethereum felt strongly enough about the adherence to the "rule" of immutability that they split from the majority of users to maintain their own separate blockchain, ethereum classic. The split of ethereum into ethereum (ETH) and ethereum classic (ETC) did not actually cause any loss to any holders of ethereum. As one commentator remarked:[149]

---

[146] Vitalik Buterin (12 March 2013), "Bitcoin Network Shaken by Blockchain Fork", *Bitcoin Magazine* at https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/ (accessed 5 April 2017). See also Gavin Andresen (20 March 2013), "BIP 50: March 2013 Chain Fork Post-Mortem" at https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki (accessed 5 April 2017). A non-technical account of this fork can be found in Popper, n 12, 192-195. Cf Smith and Atlas, n 144: "At the time of the fork, this was understood as a classical hard fork resulting from incompatibility between versions of the Bitcoin client; however, later analysis determined that the client upgrade simply caused the fork to have greater effect than it would have if all clients remained on the older version." Such forks can be caused by software behaving in a nondeterministic manner so that the same programme may behave differently each time it is run. Such behaviour can either be by design or accidental.

[147] See above, text accompanying nn 102-115.

[148] Smith and Atlas, n 144.

[149] Hertig, n 111.

> Since ethereum classic is essentially a clone of the digital currency, ether holders can now make money by making an account on the ethereum classic version of the blockchain and duplicating their balance.
>
> As ethereum classic is a replica of the original blockchain, except for a few key changes regarding The DAO transaction reversals, everyone who had tokens on ethereum at the time of the fork now has the same amount of tokens on ethereum classic. To traders, this is essentially free money.

Whether this is in fact "free money" is actually difficult to say. If values were simply computed on the basis of the value of ether at the time of the hard fork, then inasmuch as the fork did not cause its value to fall, that is certainly true. After all, "if you owned $100 of ether at the time of the fork (when it was worth roughly $12), you'd have had about 8 ETH, which means you now have 8 ETC, or an extra $16." [150] However, this view is arguably oversimplified and ignored the fall in value in ether, by almost a third, following the DAO hack.[151] While some of the loss in value is no doubt attributable to the hack itself, some of the loss is arguably the result of the market pricing in the hard fork decision.[152] Nor can it be confidently assumed that all forks would be met so sanguinely by the markets. Thus, the question of whether any legal liability ought to follow such enduring forks in the blockchain must be addressed. This is especially so as it is envisaged that there will be a hard fork in the bitcoin blockchain in the near future, in which bitcoin will split into bitcoin core (BTC) and bitcoin unlimited (BTU).[153]

It is suggested that no liability ought to follow for a number of reasons. First, insofar as such forks are mostly the result of software updates that are not unanimously (or near unanimously) adopted, it is difficult to determine who ought to be liable, even if they result in cryptocurrencies effectively changing hands on one (or more) blockchains, as was the case with the hard fork in ethereum after the DAO hack through

[150] Hertig, *ibid*.

[151] Kar and Wong, n 105.

[152] Kar and Wong, *ibid*.

[153] David Z Morris (19 March 2017), "Bitcoin Prepares for an Ugly Breakup", *Fortune* at http://fortune.com/2017/03/19/bitcoin-hard-fork/ (accessed 5 April 2017). See also Popper, n 128.

a rollback of the ethereum ledger to its state before the hack. Even if we treat all the users who updated (or refused to update, as the case may be) their software as liable for causing "loss" on one blockchain, such liability would have to have to be shared by all those users, likely thousands of users or more. Whether the law adopts a scheme of joint liability, several liability or joint and several liability, the imposition of such legal liability across the network upon users is highly impractical, especially as it is compounded by the fact that the users are spread over multiple jurisdictions. Secondly, it is difficult to conceive of an obligation on any user to update their client, much less update their client to any particular version of what is essentially open source software. Such liability, if it is to attach, would essentially amount to liability for withdrawing their computer from the claimant's desired network. However, most users do not perform any mining services or even serve as a validating node on the network. This is because most users use lightweight clients. Accordingly, it is difficult to conceive of liability attaching to anyone for failing to maintain a node (or failing to mine) on the network favoured by any particular user. Thirdly, a permanent fork in the blockchain does not erase any particular blockchain. It simply means that there are two or more, rather than one, records of transactions and accordingly, two or more blockchains. In theory, it is possible for a user to maintain his own preferred blockchain if he disagrees with the record that a particular software update will perpetuate even if no one else supported him, provided he operated a full node.

5. EXCHANGES AND INTERMEDIATION

Although bitcoins and other cryptocurrencies were often promoted through a narrative of reducing transaction costs by cutting out the middle-men,[154] many users today hold bitcoins and other cryptocurrencies through cryptocurrency exchanges. The first bitcoin exchange, Mt Gox, was set up when the computing resources required to mine bitcoin grew to the point where some users wanted more bitcoins than they could effectively mine. Mt Gox was so named because it operated on an old domain name –

[154] Cf Izabella Kaminska (17 March 2017), "But, But … I thought Bitcoin was Supposed to be Cheap?", *Financial Times*. See also Izabella Kaminska (22 March 2017), "Bitcoin's Fake News Problem", *Financial Times*.

mtgox.com – originally intended to host an exchange to buy and sell cards used in a trading card game, being the acronym for *Magic: The Gathering Online Exchange*.[155] It quickly grew to become the largest bitcoin exchange in the world until it was allegedly hacked and lost some US$460 million worth of bitcoins.[156] Although it is still unclear what exactly went wrong at Mt Gox,[157] given the frequency of hacks of such cryptocurrency exchanges, [158] it is important to determine the legal relationship between users and such exchanges given how much cryptocurrency is now held in an intermediated fashion. In this respect, the more recent hack of Bitfinex, an exchange based in Hong Kong, leading to a loss of roughly US$72 million worth of bitcoins, is instructive.

The key question is: what is the nature of the relationship between an exchange and its users? Is the account custodial in nature or is it more akin to a bank account? The legal documentation for most exchanges as to which relationship is involved is less than absolutely clear. Yet, the distinction can have dramatic consequences for end users. As a lawyer interviewed by the *Financial Times* explained, "[w]ith Bitfinex, user wallets were segregated. As a result, the relationship was seemingly more custodial in nature. In other words, the hack resulted in the theft of users' property".[159] Conversely, according to the same unnamed lawyer, "in the bank account situation, losses are necessarily socialised whereas socialising deposit box losses would be theft". However, Bitfinex appears to have taken a contrary view of their relationship with their users

[155] Popper, n 12, 51.

[156] McMillan, n 78.

[157] Jake Adelstein and Nathalie-Kyoko Stucky (19 May 2016), "Behind the Biggest Bitcoin Heist in History: Inside the Implosion of Mt Gox", *The Daily Beast* at http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html (accessed 5 April 2017).

[158] For a comprehensive academic study of the risks of bitcoin exchanges, see Moore and Christin, n 76, 25. See also Kaminska, n 76, Wong, n 76, Nakamura, n 76.

[159] Izabella Kaminska (5 August 2016), "Legal Tussle Looms for Bitcoin Holders in Hacked Bitfinex", *Financial Times*. *Contra* Clare Baldwin (6 August 2016), Bitfinex Exchange Customers to Get 36 Percent Haircut, Debt Token, *Reuters* at http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10I06H (accessed 5 April 2017).

despite the segregation of user wallets.[160]

A custodial relationship is more likely to involve a trust than a bailment given that bitcoin and other cryptocurrencies are incorporeal.[161] If the exchange holds the bitcoins on trust, then the stolen bitcoins would belong to the users whose wallets were hacked. The exchange would not ordinarily be liable to such users unless they were negligent[162] but even if they were, they would not be able to use bitcoins from other users' wallets to reimburse users whose wallets were hacked as this would entail a breach of trust[163] to those other users whose wallets were not hacked. If, however, the relationship merely entails a personal obligation to transfer a specified amount of bitcoins on demand, akin to a bank account, then any bitcoins stolen were stolen from the exchange and not its users. The exchange would remain liable to its users to the full extent of its obligations although if it were insolvent, then losses would be shared among users *pari passu*. In other words, the losses would be socialised.

It is notable that the terms of service for Bitfinex remain unclear despite their experience with the hacking. In particular, clause 1.1.21 of their Terms of Service[164] incorporates their Risk Disclosure Statement,[165] clause 4 of which is full of contradictory indications. It provides:

Exchange Risk (Counterparty Risk): Having Digital Tokens on deposit or

[160] Baldwin, *ibid*. If its assessment of the legal effect of its arrangement with its customers is wrong, then Bitfinex is exposing itself to lawsuits from customers whose wallets were *not* hacked.

[161] Norman Palmer et al, *Palmer on Bailment* (3rd ed, 2009), 1-006, but see also Chap 30.

[162] See *Morley v Morley* (1678) 2 Ch Cas 2; *Ex parte Belchier* (1754) Amb 218; 27 ER 144. Cf *Sutton v Wilders* (1872) LR 12 Eq 373. See also the statutory duty of care imposed by the Trustee Act 2000.

[163] Honest belief that this is permitted is no defence, as demonstrated most tragically in the Caleb Diplock litigation saga. The executors of Caleb Diplock distributed his estate in accordance with a bequest that they thought was valid, only to have it be declared void by the House of Lords in *Chichester Diocesan Fund v Simpson* [1944] 2 All ER 60. It is thought that the stress of the litigation caused the death of two executors, one by suicide: see C.E. Morris, "The Testament of Caleb Diplock" (1948) 65 S African LJ 578. See also *Re Diplock* [1948] Ch 465, affirmed on appeal sub nom *Ministry of Health v Simpson* [1951] AC 251.

[164] https://www.bitfinex.com/terms (accessed 5 April 2017).

[165] https://www.bitfinex.com/risk (accessed 5 April 2017).

> with any third party in a custodial relationship has attendant risks. These risks include security breaches, risk of contractual breach, and risk of loss. Participants should be wary of allowing third parties to hold their property for any reason.

The references to "custodial relationship" and "risk of loss" and "allowing third parties to hold their property" suggest a custodial trust arrangement whereas the references to "counterparty risk" and "risk of contractual breach" tend to suggest a bank account like personal obligation. Such poor drafting, perhaps intended to avoid all possible liability, is not uncommon among exchanges and will only complicate dispute resolution owing to uncertainties caused by the lack of a clear understanding of the parties' legal relations.[166]

6. CONCLUSION

Bitcoins and other cryptocurrencies have sparked a mania among investors that has been compared to the tulip mania in 17th century Netherlands.[167] It has led to much regulatory attention and thus, understandably, much of the legal analysis of bitcoins has

[166] George Priest and Benjamin Klein, "The Selection of Disputes for Litigation" (1984) 13 J Legal Stud 1, 13-17.

[167] Robinson Meyer (5 December 2013), "How Many Tulips Can You Buy With One Bitcoin?", *The Atlantic* at https://www.theatlantic.com/technology/archive/2013/12/how-many-tulips-can-you-buy-with-one-bitcoin/282062/ (accessed 5 April 2017) See also Alex Hern (4 December 2013), "Bitcoin Hype Worse than 'Tulip Mania', says Dutch Central Banker", *The Guardian* at https://www.theguardian.com/technology/2013/dec/04/bitcoin-bubble-tulip-dutch-banker (accessed 5 April 2017); Al Lewis (8 December 2013), "Tulip Bulbs for Our Time", *The Wall Street Journal*, Jean-Pierre Landau (17 January 2014), "Beware the Mania for Bitcoin, the Tulip of the 21st Century", *Financial Times*. But see also James Titcomb (28 December 2016), "Bitcoin Price at Record High Against Pound and Euro", *The Telegraph* at http://www.telegraph.co.uk/technology/2016/12/28/bitcoin-price-record-high-against-pound-euro/ (accessed 5 April 2017), Olga Kharif (24 February 2017), "Bitcoin Price Sets Record on Trump Policy Uncertainties", *Bloomberg* at https://www.bloomberg.com/news/articles/2017-02-23/bitcoin-price-sets-intraday-record-on-trump-policy-uncertainties (accessed 5 April 2017).

focused on its regulation.[168] Much less attention has been focused on how the private law might deal with bitcoin "ownership". This paper is a modest attempt to fill this gap in the legal literature. Whether bitcoins or other cryptocurrencies herald the future of money or if they remain a niche form of electronic money used predominantly by techies and geeks, it seems inevitable that the question of what private law rights a bitcoin holder has over his bitcoins will eventually have to be answered. It also seems natural that the law of property would play a central role in this enquiry. However, as this paper has demonstrated, property rights over bitcoins may well represent a truly unique and novel form of property altogether, whereby the legal right is inseparable from its registration, here on the blockchain. While the world of bitcoins and cryptocurrencies has been sustained by what has been regarded by some as blind faith and cryptographic trust, a little pixie dust in the form of private law rights will certainly not hurt in their further adoption. Clarity as to their private law nature will also help regulators determine how best they can or should be regulated.

[168] See, eg, Lawrence Trautman, "Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt Gox?" (2014) 20 Rich JL & Tech 13; Lawrence J Trautman and Alvin C Harrell, "Bitcoin Versus Regulated Payment Systems: What Gives?" (2016) 38 Cardozo L Rev 1041.